UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,667	03/23/2004	Daniel John Bricher	GCSD-1574 (51396)	1170

74701 7590 06/11/2008
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
06/11/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	**Application No.** 10/806,667	**Applicant(s)** BRICHER ET AL.
	Examiner JOSEPH PAN	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 28, 2008 has been entered.

2. Applicant's response filed on January 28, 2008 has been carefully considered. Claims 1, 13, 23, and 27 have been amended. Claims 1-34 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9, 12-19, 22-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2), hereinafter "Dhir", in view of Cheng (U.S. Pub. No. 2003/0221034 A1), and further in view of Allmond et al. (U.S. Patent No. 5,754,552), hereinafter "Allmond".

Referring to claim 1:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user network interface (see figure 8, elements 325 'host bus interface', 326 'host device interface', of Dhir),

a cryptographic processor coupled to said user network interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), and

at least one logic device for cooperating with said cryptographic processor to determine a status of said communications module (see figure 1, element 120 'programmable logic device'; and column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a <u>multi-platform</u> wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of <u>a plurality of communication protocols</u> (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

<u>Referring to claims 2, 14, 24, 28</u>:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose a plurality of interchangeable communications modules each for communicating over a different communications media (see figure 4; and abstract, lines 9-11 of Cheng).

<u>Referring to claims 3, 25, 29</u>:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the communication module comprising at least one of a type of communication module and an operating status (see figure 4, elements 'ANT2', 'PHY2'; and abstract, lines 6-11 of Cheng).

Referring to claims 4, 26:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the logic device (see abstract, lines 1-8 of Dhir).

Referring to claims 5, 15, 31:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the indicator (see column 8, lines 27-30 of Dhir).

Referring to claims 6, 16, 32:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the complex programmable logic device (CPLD) (see column 1, lines 11-16 of Dhir).

Referring to claims 7, 17, 33:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the wireless and wired communications (see figure 4, elements 'ANT2', 'PHY2'; and the abstract, lines 6-11 of Dhir).

Referring to claims 8, 18, 34:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the Ethernet (see column 2, line 18 of Dhir).

Referring to claims 9, 19:

Dhir, Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the processor and the encryption circuit (see figure 8, elements 324 'baseband processor', 321 'encryption engine' of Dhir).

Referring to claims 12, 22:

Dhir, Cheng, and Allmond teach the claimed subject matter: a communications system (see claim 1 above). They further disclose the disabling (see column 3, line 35 of Allmond).

Referring to claim 13:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user local area network interface (LAN) (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and column 6, line 66-column 7, line 3 '...These are wireless local area network specifications.', of Dhir),

a cryptographic processor coupled to said user local area network interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network LAN interface (see figure 8, element 301 'wlan transceiver' of Dhir), and

at least one logic device for cooperating with said cryptographic processor to determine at least one of a type of communications module and an operating status thereof, said at least one logic device also permitting said cryptographic processor to configure said network LAN interface (see figure 1, element 120 'programmable logic device'; and column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches an add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a <u>multi-platform</u> wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of <u>a plurality of communication protocols</u> (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

<u>Referring to claim 23</u>:

i. Dhir teaches:

A communications method comprising:

coupling a cryptographic module to a network device (see figure 8, element 321 'encryption engine' of Dhir);

providing a communications module , a network LAN interface, and at least one logic device (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver', element 300 FPGA [i.e., field programmable gate array], of Dir);

using the network LAN interface to communicate with a network (see column 6, line 66-column 7, line 3 of Dhir); and

causing the at least one logic device to cooperate with the cryptographic processor to determine a status of the communications module (see column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claim 27:

i. Dhir teaches:

A communications system comprising:

a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of said network devices (see figure 9 of Dhir);

said cryptographic device comprising a cryptographic module coupled to said at least one network device, and a communications module (see figure 8, element 321 'encryption engine', element 301 'wlan transceier' of Dhir);

said cryptographic module comprising a cryptographic processor coupled to said user network interface (see figure 8, element 321 'encryption engine', element 325 'host bus interface', element 326 'host device interface' of Dhir);

said communications module comprising a network communications interface, and at least one logic device for cooperating with said cryptographic processor to determine a status of said communications module (see figure 8, element 301 'transceiver', element 300 FPGA [i.e., field programmable gate array] of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled. Neither does Dhir specifically mention a plurality of different connectors for coupling the cryptographic module to different network devices.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that “The network connection module can be detachable from the add-on card to allow for various network configurations.” (see figure 4; and abstract, lines 9-11 of Cheng).

On the other hand, Allmond teaches a communication protocol detection system wherein Allmond discloses a plurality of different connectors for coupling the cryptographic module to different network devices (see figure 3; and column 10, line 61 - column 11, line 24 of Allmond).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Allmond into the method of Dhir to use a plurality of different connectors for coupling the cryptographic module to different network devices.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because “The network connection module can be detachable from the add-on card to allow for various network configurations.” (see figure 4; and abstract, lines 9-11 of Cheng).

The ordinary skilled person would have been motivated to have applied the teaching of Allmond into the system of Dhir use a plurality of different connectors for coupling the cryptographic module to different network devices, because Dhir teaches a method for providing a multi-platform wireless local area network (see column 3, lines 1-2 of Dhir, emphasis added). Allmond teaches a networking device to automatically detecting and interconnecting network devices, each operating according to any one of a plurality of communication protocols (see column 1, lines 16-20 of

Allmond, emphasis added). Therefore, Allmond's teaching could enhance Dhir's system.

Referring to claim 30:

Dhir, Cheng, and Allmond teach the claimed subject matter: a communications system (see claim 27 above). They further disclose configuring the network communications (see column 1, lines 7-9 of Dhir).

5. Claims 10-11, 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2) in view of Cheng (U.S. Pub. No. 2003/0221034 A1), further in view of Allmond et al. (U.S. Patent No. 5,754,552), and further in view of Klein (U.S. Patent No. 6,857,076 B1).

Referring to claims 10, 20:

i. Dhir , Cheng, and Allmond teach the claimed subject matter: a cryptographic device (see claim 1 above). Dhir further discloses the encryption engine (see figure 8, element 321 ‘encryption engine’ of Dhir).

However, they do not specifically mention the data buffer.

ii. Klein teaches data security for digital data storage, wherein Klein discloses the data buffer (see column 5, lines 57-67 of Klein)

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Klien into the method of Dhir , Cheng, and Allmond to utilize the data buffer for encryption.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Klien into the system of Dhir , Cheng, and Allmond to utilize the data buffer for encryption, because data buffer can be used to store data during encryption process.

Referring to claims 11, 21:

Dhir, Cheng, Allmond, and Klein teach the claimed subject matter: a communications system (see claim 10 above). They further disclose the tampering (see column 7, line 44-45 of Klein).

Response to Arguments

6. Applicant's arguments, filed on January 28, 2008, have been fully considered. The amended independent claims now contain the claim limitation: "comprising a plurality of different connectors for coupling the cryptographic module to different network devices". Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Allmond.

Applicant argues:

"Applicants further submit that the Examiner's combination of Dhir et al. and Cheng is improper, as a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. to arrive at the claimed invention. More particularly, Dhir et al. is directed to a programmable integrated circuit for a WLAN. The communications module and the cryptographic module are purposely on **a single FPGA (300) chip**, as illustrated in Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single EPGA." (see page 4, 2nd paragraph, Applicant's Arguments/Remarks, emphasis added)

Examiner maintains:

Dhir discloses "Referring to FIG. 7, there is shown an exemplary embodiment of FPGA 300 program in accordance with one or more aspects of the present invention. In this embodiment, a **separate transceiver** 301 integrated circuit [i.e., the communication module], namely not embedded in FPGA 300, is coupled to FPGA 300 [i.e., the cryptographic module], as is program memory 312. In this embodiment, a direct interface between **separate transceiver** 301 and FPGA 300 may be employed for direct interaction between transceiver 301 and FPGA 300." (see column 7, lines 48-56 of Dhir). Thus, Dhir discloses that the transceiver [i.e., the communications module] is coupled to the PFGA [i.e., the cryptographic module]. Therefore, a person having ordinary skill in the art would turn to Cheng to combine with Dhir et al. to arrive at the claimed invention.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
June 2, 2008
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135